REMARKS

The misspelling on page 4 has been corrected.

A new title has been supplied as suggested.

Claim 8 has been amended to make it clear that the secret key is known to both the authentication authority and the document checker. Basis for this can be found on page 2, lines 16-17, of the specification. This clearly overcomes the objection that claim 8 is not grammatical.

Claim 8 has also been amended to make it clear that the secret key is not known to the document producer. This must clearly be the case, since otherwise the document producer would be able to authenticate their own documents.

Claim rejections – 35 USC §112

Claim 8 has been amended as mentioned above.

Claim 12 has been amended to correct an error in terminology, by replacing "certificate" with "document".

It is believed that these amendments clearly overcome the rejections of claims 8 and 12 as indefinite.

Claim rejections – 35 USC §102

It is respectfully submitted that claims 1 and 13, as amended, are clearly distinguished from the prior art and in particular from the Kocher reference (U.S. Patent no 6,188,766).

Claim 1 defines a method for authenticating a printed document in which a document producer sends information to be included in a document to an authentication authority. The authentication authority checks whether the document producer is authorized to produce the document and, if so, cryptographically generates an authentication code from this information, and sends the authentication code back to the document producer. Upon receipt of the authentication code from the authentication authority, the document producer then prints the document, including both the information and the authentication code. Upon presentation of the document for authentication, a document checker cryptographically checks the authentication code against the information in the document to determine whether the printed document is authentic.

Kocher describes an apparatus and method for confirming, timestamping and archiving printer and telecopier documents. A user sends a document to a trusted timestamping service (TTS) via facsimile. The TTS computes a timestamp and electronically archives the document with the timestamp. The TTS then sends a receipt to the user, via facsimile, confirming the transaction. (See column 3, lines 33-55). The receipt includes a copy (typically reduced size) of the document images so that the user can confirm that the document images were received properly. The receipt also includes a document identification value DIV or telecopier transmission identifier TTI to identify the document. (See column 8, lines 22-30). When a requester wishes to verify the integrity of the document, they contact the TTS, quoting the DIV/TTI of the document. (See column 10, lines 10-15). The TTS uses this DIV/TTI to retrieve the archived document, and sends a copy back to the requester, along with the timestamp.

It can be seen that the method as proposed by Kocher is fundamentally different from that of the present invention.

First, it should be noted that in Kocher, the trusted timestamping service (TTS) does not return an authentication code to the document producer as required by the present invention. The TTS returns a timestamp, and a document identifier (DIV/TTI), but clearly neither of these can be construed as an authentication code, since neither actually confirms the authenticity of the document.

Since Kocher's TTS does not return any authentication code to the document producer, then clearly the document producer cannot print the document including an authentication code, as required by the present invention.

Moreover, it should be noted that in Kocher, the trusted timestamping service (TTS) does not check whether the document producer is authorized to produce the document, as required by the present invention. The TTS merely checks whether the user is authorized to use the TTS service (see column 7, lines 42-46). This is not the same thing: even if a user is authorized to use the TTS service, they would not necessarily be authorized to print a vehicle test certificate or a medical prescription, for example.

Furthermore, it should be noted that there is absolutely no suggestion in Kocher that a document checker can determine whether the printed document is authentic by cryptographically checking an authentication code against information in the document, as required by the present invention. On the contrary, in Kocher, verification of the document requires the requester to contact the trusted timestamping service (TTS). The TTS merely returns a copy of the archived document and its timestamp to the requester, and presumably the requester then has to visually compare the archived copy with the "original" document, to ensure that the original has not been tampered with and its date has not been altered.

Regarding claim 2, it is clear that Kocher's bar code (Fig. 4) contains the timestamp, not an authentication code. (See column 9, line 14). Therefore, it is submitted that claim 2 is clearly distinguished from the Kocher reference.

Regarding claims 3 - 5, it is respectfully submitted that there is absolutely no suggestion in Kocher of including a pre-printed serial number in a document, and of using this number in generating an authentication code. The "serial numbers" mentioned in Kocher, column 7, lines 31-32 are clearly facsimile serial numbers, and are not derived from any numbers pre-printed in the document. Similarly, the "serial numbers" mentioned in Kocher, column 7, line 40 are clearly device serial numbers, not document serial numbers.

Regarding claims 6 – 10 , it is pointed out that the "authenticity code" referred to in Kocher, for example in column 6, line 28, is clearly used by the trusted timestamping service (TTS) to verify that the archived electronic copy has not been tampered with (see column 6, lines 33-34), not to authenticate the printed document. Hence, it is respectfully submitted that Kocher clearly does not teach any steps for checking the authenticity of a printed document, by comparing an authentication code in that printed document with a check code generated from information in the printed document, as claimed.

Furthermore, it is respectfully pointed out that the cryptographic operations referred to in Kocher, for example in column 7, lines 46-56, are clearly for protecting the timestamp in the electronically archived document, and are not for generating an authentication code that can be used to authenticate the printed document.

Regarding claim 8 in particular, it is submitted that there is no suggestion in Kocher of using a secret key known to both the authentication authority and the document checker, but not known to the document producer, to generate an authentication code. The keys referred to in Kocher, column 6, lines 34-49 must clearly be known only to the trusted timestamping service (TTS) and not to any other entity.

Regarding claims 13 – 15, as noted by the examiner, these are apparatus claims corresponding to the method claims, and it is respectfully submitted that the above arguments apply equally to these claims.

Claim rejections – 35 USC §103

Claim 12 was rejected as being unpatentable over Kocher in view of the Verisign Certification Practice Statement version 1.2.

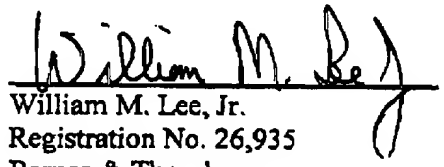
Since the system described in the Kocher reference has been shown to be completely different in principle from that of the present invention as defined in independent claim 1, from which claim 12 is dependent, it is respectfully submitted that this ground of rejection is moot.

Conclusion

In summary, it is submitted that this application is now clearly in order for allowance and such action is respectfully solicited.

December 17, 2003

Respectfully submitted,



William M. Lee, Jr.
Registration No. 26,935
Barnes & Thornburg
P.O. Box 2786
Chicago, Illinois 60690-2786
(312) 214-4800
(312) 759-5646 (fax)